

Privacy Tip of the Week:
West Virginia Executive Branch

Spyware, Malware, Adware and Other Naughty Programs

Question:

Okay, so I'm not as tech savvy as some of my friends. I feel like I'm in a sci-fi movie when I hear them talking about spyware and malware and pop-ups and cookies. Help me understand this stuff!

Answer:

"Spyware" refers to software that is surreptitiously installed on your computer. Some spyware programs may deliver pop-up ads or monitor your online activity. Truly malicious spyware (malware) may even capture your keystrokes, so that thieves can steal your passwords and other sensitive personally identifiable information (PII).

Spyware and malware can cause computer problems. Because these programs run in the background, they use processing resources and cause computers to be slow. They can also create privacy and security risks, especially if you are not aware that PII is being collected by an unauthorized third party.

According to US-CERT's Cyber Security Tip ST04-016 the following symptoms may indicate that spyware or malware is installed on your computer:

- ✓ You are subjected to endless pop-up windows,
- ✓ You are redirected to web sites other than the one you typed into your browser,
- ✓ New, unexpected toolbars appear in your web browser,
- ✓ New, unexpected icons appear in the task tray at the bottom of your screen,
- ✓ Your browser's home page suddenly changed,
- ✓ The search engine your browser opens when you click "search" has been changed,
- ✓ Certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form),
- ✓ Random Windows error messages begin to appear, or
- ✓ Your computer suddenly seems very slow when opening programs or processing tasks (saving files, etc.).

What do you do if you think you may have spyware or malware installed on your computer? Contact the OT Service Desk. Service Desk personnel can use tools to scan your computer, detect, and remove any naughty software.

If you think you may have spyware or malware on a personal machine, there are many products that you can use, some are even free. Popular products include Lavasoft's Ad-Aware, Microsoft's Window Defender, Webroot's SpySweeper, MalwareBytes® and Spybot Search and Destroy.

To avoid unintentionally installing spyware, here are some good security practices recommended by US-CERT:

- ✓ **Don't click on links within pop-up windows** - Because pop-up windows are often a product of spyware, clicking on the window may install spyware software on your computer. To close the pop-up window, click on the "X" icon in the title bar instead of a "close" link within the window.
- ✓ **Choose "no" when asked unexpected questions** - Be wary of unexpected dialog boxes asking whether you want to run a particular program or perform another type of task. Always select "no" or "cancel," or close the dialog box by clicking the "X" icon in the title bar.
- ✓ **Be wary of free downloadable software** - There are many sites that offer customized toolbars or other features that appeal to users. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- ✓ **Don't follow email links claiming to offer anti-spyware software** - Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.
- ✓ **Don't use the "preview pane" in Outlook or other mail programs** - This actually opens an email and may subject you to risk of infection. It is better to delete an email from an unknown source and risk missing a message than to risk infection.

As an additional good security practice, especially if you are concerned that you might have spyware or malware on your machine and want to minimize the impact, consider taking the following action:

- ✓ **Adjust your browser preferences to limit pop-up windows and cookies** - Pop-up windows are often generated by some kind of scripting or active content. Adjusting the settings within your browser to reduce or prevent scripting or active content may reduce the number of pop-up windows that appear. Some browsers offer a specific option to block or limit pop-up windows. Certain types of cookies are sometimes considered spyware because they reveal what web pages you have visited. You can adjust your privacy settings to only allow cookies for the web site you are visiting.

Contact the OT Service Desk, your IT Department or your Privacy Officer if you need any help with spyware or your computer security settings!